

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 2001111543
PUBLICATION DATE : 20-04-01

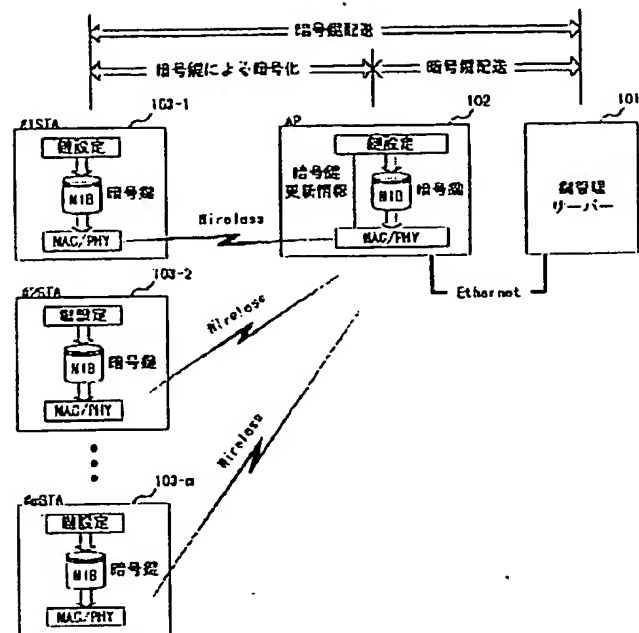
APPLICATION DATE : 07-10-99
APPLICATION NUMBER : 11287262

APPLICANT : NEC CORP;

INVENTOR : MORIMOTO SHINICHI;

INT.CL. : H04L 9/16 H04L 9/08 H04L 12/28

TITLE : CRYPTOGRAPHIC KEY UPDATE
SYSTEM OF RADIO LAN AND
UPDATING METHOD THEREFOR



ABSTRACT : PROBLEM TO BE SOLVED: To provide a cryptographic key update system and an updating method, capable of applying WEP of IEEE802.11 to a radio LAN system having many APs and STAs.

SOLUTION: This cryptographic key update system is constituted, so that a cryptographic key to be used for ciphering radio communication among all AP and STAs is defined as one set (k pieces), managed unitarily and distributed to each AP and STA, when the cryptographic key is updated by a key management server by providing the key management server connected with the AP by LAN.

COPYRIGHT: (C)2001,JPO

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-111543

(P2001-111543A)

(43)公開日 平成13年4月20日(2001.4.20)

(51)Int.Cl. ⁷	識別記号	F I	テームト*(参考)
H 0 4 L	9/16	H 0 4 L 9/00	6 4 3 5 J 1 0 4
	9/08		6 0 1 E 5 K 0 3 3
	12/28		6 0 1 A
			6 0 1 B
		11/00	3 1 0 B
		審査請求 有	請求項の数19 O L (全 14 頁)

(21)出願番号 特願平11-287262

(22)出願日 平成11年10月7日(1999.10.7)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 森本 伸一

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100082935

弁理士 京本 直樹 (外2名)

Fターム(参考) 5J104 AA01 AA16 AA34 EA01 EA18

MA05 NA02 NA37 PA00 PA07

5K033 AA08 BA13 CB01 CB03 CC04

DA01 DA17 DB10 DB12 DB14

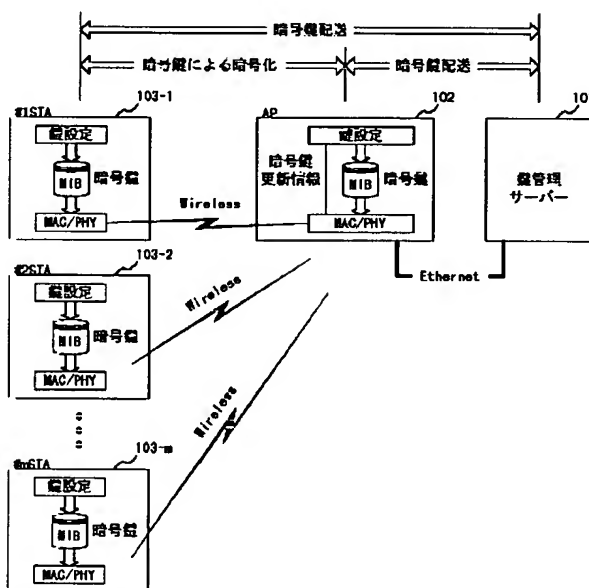
EC01

(54)【発明の名称】 無線LANの暗号鍵更新システム及びその更新方法

(57)【要約】

【課題】 複数のAP、多数のSTAを有する無線LANシステムに、IEEE802.11のWEPを適用できる、暗号鍵更新方式及び更新方法を提供する。

【解決手段】 APとLAN接続された鍵管理サーバーを有し、全てのAPとSTAの間の暗号化無線通信に使用する暗号鍵を1組(k個)とし、一元管理するとともに、鍵管理サーバーにて暗号鍵を更新すると、各AP、及び各STAに配送するよう構成している。



【特許請求の範囲】

【請求項1】LAN上に1以上の無線アクセスポイント装置（AP）を有し、前記APは1以上の無線アクセス端末装置（STA）と無線接続し、前記STAとの間でデータを暗号化して通信（暗号化通信）する無線LANの暗号鍵更新システムにおいて、前記APとLAN接続された鍵管理サーバ装置（SV）は前記APと前記STAの暗号化通信に使用する k 個（ k は1以上）の暗号鍵を記憶するSV記憶手段と、前記暗号鍵を生成し前記SV記憶手段に格納する暗号鍵生成手段とを有し、前記SVは、前記SV暗号鍵生成手段にて前記暗号鍵を生成して前記SV記憶手段に格納し、予め設定された条件に従って前記暗号鍵生成手段を制御して前記SV記憶手段に記憶した前記暗号鍵を更新し、更新した前記暗号鍵を前記APと前記STAに配信する、ことを特徴とする、無線LANの暗号鍵更新システム。

【請求項2】前記SVは、前記SV記憶手段に記憶された前記暗号鍵を更新する時、前記暗号鍵生成手段にて1時に暗号鍵を1個生成し更新する、ことを特徴とする、請求項1に記載の無線LANの暗号鍵更新システム。

【請求項3】前記SVは、前記SV記憶手段に記憶された前記暗号鍵を更新する時、前記暗号鍵生成手段にて1時に前記暗号鍵を1個生成し、前記SV記憶手段に記憶された k 個の暗号鍵を所定間隔で1個ずつ順次に更新する、ことを特徴とする、請求項1に記載の無線LANの暗号鍵更新システム。

【請求項4】前記SVは、前記SV記憶手段に記憶された k 個の前記暗号鍵の内、（ $k-1$ ）個の暗号鍵については所定間隔（間隔1）で1個ずつ順次更新し、他の1個は（ $k-1$ ）個の暗号鍵より長い間隔（間隔2）で更新する、ことを特徴とする、請求項1に記載の無線LANの暗号鍵更新システム。

【請求項5】前記APは、前記SVの更新した第 n 番（ n は、 $1 \leq n \leq k$ ）の暗号鍵を配信されると前記APの記憶管理する第 n 番の暗号鍵を更新する手段と、第 n 番以外の暗号鍵を用いて暗号鍵更新通知伝文を暗号化して前記STAに通知する手段とを有し、前記STAは、前記APから前記暗号鍵更新通知伝文を受けるとSTA暗号鍵更新要求伝文を生成する手段と、前記暗号鍵更新通知伝文と同一の暗号鍵を用いて前記STA暗号鍵更新要求伝文を暗号化して前記APに通知する手段とを有し、前記APは、さらに、前記STAから前記STA暗号鍵更新要求伝文を受けると前記SVへSTA暗号鍵更新要求を通知する手段を有し、前記SVは、さらに、前記APから前記STA暗号鍵更新要求を受けると前記STA宛て暗号鍵配送の可否を判断する手段と、可と判断した場合に前記APへ前記STA宛て暗号鍵を配送する手段とを有する、ことを特徴とする、請求項2乃至4の内、いずれか1に記載の無線LANの暗号鍵更新システム。

【請求項6】前記APは、前記SVの更新した第 n 番（ n は、 $1 \leq n \leq k$ ）の暗号鍵を配信されると前記APの記憶管理する第 n 番の暗号鍵を更新する手段と、前記APの記憶管理する k 個の暗号鍵の内、最初に更新された暗号鍵を用いて暗号鍵更新通知伝文を暗号化して前記STAに通知する手段とを有し、前記STAは、前記APから前記暗号鍵更新通知伝文を受けるとSTA暗号鍵更新要求伝文を生成する手段と、前記暗号鍵更新通知伝文と同一の暗号鍵を用いて前記STA暗号鍵更新要求伝文を暗号化して前記APに通知する手段とを有し、前記APは、さらに、前記STAから前記STA暗号鍵更新要求伝文を受けると前記SVへSTA暗号鍵更新要求を通知する手段を有し、前記SVは、前記APから前記STA暗号鍵更新要求を受けると前記STA宛て暗号鍵配送の可否を判断する手段と、可と判断した場合に前記APへ前記STA宛て暗号鍵を配送する手段とを有する、ことを特徴とする、請求項2乃至4の内、いずれか1に記載の無線LANの暗号鍵更新システム。

【請求項7】前記APは、さらに、前記SVから前記STA宛て暗号鍵を配送されるとSTA暗号鍵配送伝文を生成する手段と、第 n 番以外の暗号鍵を用いて前記STA暗号鍵配送伝文を暗号化して前記STAに通知する手段とを有し、前記STAは、さらに、前記APから前記STA暗号鍵配送伝文にて第 n 番の暗号鍵を配送されると前記STAの記憶管理する第 n 番の暗号鍵を更新する手段を有する、ことを特徴とする、請求項5、または6に記載の無線LANの暗号鍵更新システム。

【請求項8】前記APは、さらに、前記SVから前記STA宛て暗号鍵を配送されるとSTA暗号鍵配送伝文を生成する手段と、APの記憶管理する k 個の暗号鍵の内、最初に更新された暗号鍵を用いて前記STA暗号鍵配送伝文を暗号化して前記STAに通知する手段とを有し、前記STAは、さらに、前記APから前記STA暗号鍵配送伝文にて第 n 番の暗号鍵を配送されると前記STAの記憶管理する第 n 番の暗号鍵を更新する手段を有する、ことを特徴とする、請求項5、または6に記載の無線LANの暗号鍵更新システム。

【請求項9】前記STAは、所定の要因を検出すると、STA暗号鍵一括更新要求伝文をAPへ通知する手段を有し、前記APは、前記STAから前記STA暗号鍵一括更新要求伝文を受けると前記SVへSTA暗号鍵一括更新要求を通知する手段を有し、前記SVは、前記APから前記STA暗号鍵一括更新要求を受けると前記STA宛て暗号鍵一括配送の可否を判断する手段と、可と判断した場合に前記APへ前記STA宛て暗号鍵を一括配送する手段とを有し、前記APは、さらに、前記SVから前記STA宛て暗号鍵の一括配送を受けるとSTA暗号鍵一括配送伝文を生成して前記STAに通知する手段を有し、前記STAは、さらに、前記APから前記STA暗号鍵一括配送伝文を受けると前記STAの記憶する

暗号鍵を一括して更新する手段を有する、ことを特徴とする、請求項1乃至4の内、いずれか1に記載の無線LANの暗号鍵更新システム。

【請求項10】LAN上に1以上の無線アクセスポイント装置（AP）を有し、前記APは1以上の無線アクセス端末装置（STA）と無線接続し、前記STAとの間でデータを暗号化して通信（暗号化通信）する無線LANの暗号鍵更新方法において、前記APとLAN接続された鍵管理サーバー装置（SV）は前記APと前記STAの暗号化通信に使用する k 個（ k は1以上）の暗号鍵を生成するとともに記憶管理し、予め設定された条件に従って更新し、更新した前記暗号鍵を前記APと前記STAに配信する、ことを特徴とする、無線LANの暗号鍵更新方法。

【請求項11】前記SVは、前記SVの記憶管理する k 個の前記暗号鍵を更新する時、 k 個の暗号鍵の内、1時に1個を更新する、ことを特徴とする、請求項10に記載の無線LANの暗号鍵更新方法。

【請求項12】前記SVは、前記SVの記憶管理する k 個の前記暗号鍵を更新する時、 k 個の暗号鍵を所定間隔で1個ずつ順次に更新する、ことを特徴とする、請求項10に記載の無線LANの暗号鍵更新方法。

【請求項13】前記SVは、前記SVの記憶管理する k 個の前記暗号鍵の内、（ $k-1$ ）個の暗号鍵については所定間隔（間隔1）で1個ずつ順次に更新し、他の1個は（ $k-1$ ）個の暗号鍵より長い間隔（間隔2）で更新する、ことを特徴とする、請求項10に記載の無線LANの暗号鍵更新方法。

【請求項14】前記APは、前記APの記憶管理する第 n 番（ n は、 $1 \leq n \leq k$ ）の暗号鍵を更新してから次に暗号鍵を更新するまでの間、前記APの記憶管理する第 n 番以外の任意の暗号鍵を用いて前記STAと暗号化通信する、ことを特徴とする、請求項11乃至13の内、いずれか1に記載の無線LANの暗号鍵更新方法。

【請求項15】前記APは、前記APの記憶管理する第 n 番（ n は、 $1 \leq n \leq k$ ）の暗号鍵を更新してから次に暗号鍵を更新するまでの間、前記APの記憶管理する第 n 番以外の（ $k-1$ ）個の暗号鍵を順次用いて前記STAと暗号化通信する、ことを特徴とする、請求項11乃至13の内、いずれか1に記載の無線LANの暗号鍵更新方法。

【請求項16】前記APは、前記APの記憶管理する k 個の暗号鍵の内、最初に更新された暗号鍵を用いて前記STAと暗号化通信する、ことを特徴とする、請求項11乃至13の内、いずれか1に記載の無線LANの暗号鍵更新方法。

【請求項17】前記STAは、前記STAの記憶管理する第 n 番以外の（ $k-1$ ）個の暗号鍵の内、任意の暗号鍵を用いて前記APと暗号化通信する、ことを特徴とする、請求項14乃至16の内いずれか1に記載の無線LANの暗号鍵更新方法。

ANの暗号鍵更新方法。

【請求項18】前記STAは、前記STAの記憶管理する第 n 番以外の（ $k-1$ ）個の暗号鍵を順次用いて前記APと通信する、ことを特徴とする、請求項14乃至16の内いずれか1に記載の無線LANの暗号鍵更新方法。

【請求項19】前記STAは、前記STAの記憶管理する k 個の暗号鍵の内、最後に更新された暗号鍵を用いて前記APと通信する、ことを特徴とする、請求項14乃至16の内いずれか1に記載の無線LANの暗号鍵更新方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データを暗号化して無線通信する無線LANシステムに関し、特にWEPメカニズムによる暗号化を用いた無線LANシステムにおける暗号鍵更新システム及びその更新方法に関する。

【0002】

【従来の技術】従来、無線LANシステムの普及に伴って、通信データの保護、すなわち、無線アクセスのセキュリティの確保が望まれていた。

【0003】近年、屋外用途だけでなく、屋内向けにも無線LANシステムの導入が進んでいる。例えば、構内にアクセスポイント（AP：固定の基地局）を設置し、フロア内に設置する端末装置に送受信装置（STA）を接続してAPとの間を無線化し、端末装置の配置変更の容易化、携帯型端末装置の常出入に関する利便性向上を図るなどの例が増えている。

【0004】このようなシステムにおいては、例えば外来者の持ちこむ携帯型無線端末装置や、屋外へ漏洩する電波を傍受可能な外部の無線端末装置に対して、通信データを保護する必要がある。

【0005】無線通信におけるデータ保護の方式としては、暗号化を採用するものが一般化しつつある。無線データ通信における暗号化方式については、これまでIEEEで標準化の検討が進められてきた。

【0006】現在のところ、無線区間の暗号化及び認証の方式としては、IEEE802.11において、WEP（The Wired Equivalent Privacy algorithm）メカニズムを使用した、Shared Key認証（共通鍵）方式が採用されている。

【0007】図6（a）は、IEEE802.11の8.2.3章に記載されている、WEPメカニズムによる暗号化方式を示すブロック図、（b）は、同じく復号化方式を示すブロック図である。

【0008】図6（a）に示すように、WEPメカニズムによる暗号化方式は、Seed生成手段601、暗号化手段602、誤り検出符号生成手段603、誤り検出符号付加手段604、及び暗号文生成演算手段605よ

り構成され、暗号化メッセージ606を出力する。暗号化手段602は、RC4アルゴリズムにより構成されている。

【0009】図6(a)の動作についてはIEEE802.11ドラフト中に記載があるので説明を省略するが、図6(a)の暗号化方式は、イニシャライゼーションベクタ(IV)、秘密鍵(Secret Key)、及び通信データ(Plaintext)を入力し、IVと暗号文(Ciphertext)を出力する。

【0010】図6(b)に示す、WEPメカニズムによる復号化方式は、Seed生成手段611、暗号化手段612、復号化演算手段613、符号分離手段614、誤り検出符号生成手段615、誤り検出符号比較手段616により構成されている。暗号化手段612は、RC4アルゴリズムにより構成されている。

【0011】図6(b)の復号化方式は、受信した暗号化メッセージ606からIVと暗号文を入力し、復号方式側で予め設定され、記憶している秘密鍵を使用して復号演算処理を行う。この結果、復号した明文(Plaintext)と、誤り検出符号(ICV)比較結果を出力する。

【0012】図7は、図6(a)から(b)へ伝送される暗号化メッセージ606の構成を示す。暗号化メッセージ606の構成は、拡張WEPフレームと称される。図7において各構成要素中に示す数字は、Octets(8ビット、以下「バイト」と記す)を単位としている。拡張WEPフレームは4バイトのIV701と、1バイト以上のデータ(PDU)702、4バイトのICV703により構成されている。拡張WEPフレームのデータ702、及びICV703は暗号化(Encrypt)され、IV701は暗号化されずに伝送される。

【0013】IV701は、暗号化に使用する暗号鍵の識別情報を含んでいる。すなわち、図示する様に、IV701は3バイトのイニシャライズベクター本体704に、6ビットのパッド705と、2ビットの鍵ID(Key ID)706とからなる1バイトの情報707を付加して構成されている。

【0014】この鍵ID706は2ビットの情報で構成されているので、4つまでの暗号鍵を識別することができる。従って、IEEE802.11の、WEPメカニズムを使用した暗号化方式においては、4つまでの暗号鍵を識別管理し、運用することができる。

【0015】ところで、従来この種の無線通信に用いられる暗号化復号化技術、あるいは暗号通信装置としては、様々なものが提案されている。

【0016】例えば、特開平11-196081号公報を参照すると、送信局と受信局とからなる暗号通信装置に適用できる暗号鍵の更新技術が開示されている。特開平11-196081号公報の発明によれば、暗号化によるデータ通信の手順は次のようである。

【0017】すなわち、まず、送信側にて予備鍵を生成する。次に送信側にて暗号鍵を用いて暗号化した伝文により、予備鍵を送信する。送受信双方で予備鍵を暗号鍵として更新し、以降これを用いて暗号化、復号化を行い、データを通信する。

【0018】この発明を実施するための構成の特徴としては、第1に予備鍵の記憶手段を有していること、第2に暗号鍵の記憶手段を有していること、第3に予備鍵を送信局が生成していることが挙げられる。

【0019】

【発明が解決しようとする課題】ところで、上記従来の暗号通信装置では、第1に鍵の管理を1対1で行っている。このため、そのままでは1対多のシステムへの応用が難しいという問題を有していた。

【0020】また、多くのSTAと、APとの間で無線アクセス環境を提供するシステムへの応用を考えた場合、APは、多くの端末のアクセスに使用する鍵を管理することとなる。例えばn台のSTAを有するシステムでは、APはn台分の暗号鍵を記憶管理する手段が必要となるので、回路規模が増大するとともに、処理の負荷が増大するという問題を有していた。

【0021】また、可搬型のSTAを使用者が持ち運んで移動したり、フロアのレイアウト変更などによってSTAが移設されることによって、それまでとは異なるAPにアクセスすることとなった場合には、STAとAPとで記憶管理している暗号鍵が不一致となり、通信できなくなるという問題を有していた。

【0022】さらに、特開平11-196081号公報の発明を1対多のシステムへ応用することを考えた場合、APは各STAに予備鍵を配送し、全てのSTAに予備鍵が行き渡った後、配布した予備鍵を暗号鍵として更新する手順が考えられる。しかしながら、このような手順で暗号鍵を更新しようとしても、全てのSTAが常時APにアクセスしているとは限らない状況においては、配送した予備鍵を暗号鍵に更新することができなくなる場合があるという問題を有していた。

【0023】従って、本発明の第1の目的は、多数のSTAと、APの間で行われる暗号化通信システムに適用可能な暗号通信装置を提供することにある。

【0024】また、多数のSTAがAPと通信する暗号化通信システムにおいて、容易に暗号鍵を生成、管理可能な暗号通信方式を提供することを第2の目的とする。

【0025】また、可搬型のSTAを移動したり、STAが移設されて、それまでとは異なるAPにアクセスすることとなった場合にも、新たなAPと、問題無くアクセスすることのできる暗号通信方式を提供することを第3の目的とする。

【0026】さらに、システムに属する全てのSTAがAPにアクセス可能な状態で無い場合にも随時暗号鍵を更新することで暗号化通信の信頼性を確保するとともに

に、暗号鍵の更新されなかったSTAに対する暗号鍵更新手順を設け、高い運用効率を有する暗号通信方式を提供することを第4の目的とする。

【0027】

【課題を解決するための手段】上記の目的を達成するため、本発明の暗号鍵更新方式は、1以上のAPとLAN接続された鍵管理サーバーを有し、全てのAPとSTAの間の暗号化無線通信に使用する暗号鍵を1組(k個)とし、一元的に管理するとともに、各AP、及び各STAに配送するよう構成している。

【0028】本発明の暗号鍵更新方式のAPは、k個の暗号鍵記憶手段を有し、鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照してSTAと暗号化通信するよう構成している。

【0029】本発明の暗号鍵更新方式のSTAは、k個の暗号鍵記憶手段を有し、AP経由で鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照してAPと暗号化通信するよう構成している。

【0030】本発明の暗号鍵更新方式のSTAは、暗号鍵記憶手段に記憶された全ての暗号鍵がAPと一致しない場合、AP経由で鍵管理サーバーに、暗号鍵の一括更新を要求し、鍵管理サーバーから暗号鍵を一括配送されるとSTAにて記憶管理していた暗号鍵を更新し、これを参照してAPと暗号化通信するよう構成している。

【0031】本発明の暗号鍵更新方法は、1以上のAPとLAN接続された鍵管理サーバーを有し、全てのAPとSTAの間の暗号化無線通信に使用する暗号鍵を1組(k個)とし、一元的に管理するとともに、各AP、及び各STAに配送する。

【0032】本発明の暗号鍵更新方法のAPは、k個の暗号鍵記憶手段を有し、鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照してSTAと暗号化通信する。

【0033】本発明の暗号鍵更新方法のSTAは、k個の暗号鍵記憶手段を有し、AP経由で鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照してAPと暗号化通信する。

【0034】本発明の暗号鍵更新方法のSTAは、暗号鍵記憶手段に記憶された全ての暗号鍵がAPと一致しない場合、AP経由で鍵管理サーバーに、暗号鍵の一括更新を要求し、鍵管理サーバーから暗号鍵を一括配送されるとSTAにて記憶管理していた暗号鍵を更新し、これを参照してAPと暗号化通信する。

【0035】

【発明の実施の形態】以下に、本発明の実施の形態について、図面を参照して説明する。

【0036】図1は本発明の実施の形態による無線LANシステムの構成を示すブロック図である。図1に示す、本発明による無線LANシステムは、鍵管理サーバー101、AP102、複数(m台)のAP(#1STA

A103-1、#2STA103-2、…#mSTA103-m)より構成されている。

【0037】AP102とSTA103との間はIEEE802.11による無線(Wireless)LAN接続にて構成されている。

【0038】STAとAPとの間のデータ通信では、WEPメカニズムを使用した暗号化方式を用いる。WEPメカニズムを使用した暗号化方式では、STAとAPは、それぞれ4個の暗号鍵を記憶管理し、暗号化、復号化を行う。

【0039】図1の鍵管理サーバー101は、AP102とSTA103との間の無線区間において、暗号化に使用する暗号鍵を生成、管理する。鍵管理サーバーは新たな鍵を生成すると、AP102、STA103へ配送する。

【0040】AP102は、鍵管理サーバー101から暗号鍵を配送されると、STA103との通信に使用する暗号鍵を更新し、記憶管理するとともに、STA103に暗号鍵の更新を通知する。

【0041】STA103は、鍵管理サーバー101からAP102を経由して配送された暗号鍵を記憶管理し、暗号鍵を使用してAPと通信する。

【0042】図2は、AP102の構成を示すブロック図である。図2に示す、本発明によるAP102は、制御手段201、暗号鍵設定手段202、第1鍵記憶手段203、第2鍵記憶手段204、第3鍵記憶手段205、第4鍵記憶手段206、鍵選択手段207、鍵ID生成手段208、IV生成手段209、平文入力手段210、WEP暗号化手段211、暗号文送出手段212、暗号文入力手段213、WEP復号手段214、平文出力手段215、及び、鍵ID抽出手段216より構成されている。

【0043】ここで、WEP暗号化手段211は、図6(a)にて説明した、IEEE802.11のWEPによる暗号化方式にて構成されている。また、WEP復号化手段214は、図6(b)にて説明したIEEE802.11のWEPによる復号化方式にて構成される。

【0044】図2に示す、第1乃至第4の鍵記憶手段203乃至206は、図1にも示すように、MIBと称されるバッファにより構成することができる。MIBはソフトウェアによって書換えることは可能であるが、ソフトウェアによって読み出すことは不可能な構造を持つ、情報秘匿性の高い記憶手段である。

【0045】尚、図2に示す暗号鍵生成手段200は、鍵管理サーバーに含まれる。

【0046】図3は、STA103の構成を示すブロック図である。図3に示す、本発明によるSTA103は、制御手段301、暗号鍵設定手段302、第1鍵記憶手段303、第2鍵記憶手段304、第3鍵記憶手段305、第4鍵記憶手段306、鍵選択手段307、鍵

ID生成手段308、IV生成手段309、平文入力手段310、WEP暗号化手段311、暗号文送出手段312、暗号文入力手段313、WEP復号化手段314、平文出力手段315、及び、鍵ID抽出手段316より構成されている。図3に示す、第1乃至第4の鍵記憶手段303乃至306は、図2に示した鍵記憶手段と同様、MIBにより構成することができる。

【0047】図4、図5は、本発明による無線LANシステムにおける、暗号鍵の更新手順を示すシーケンスチャートである。

【0048】図4は、通常の暗号鍵更新手順を示している。すなわち、STAとAPは、互いに同じ暗号鍵を記憶管理している状態で、鍵管理サーバが新たな暗号鍵を生成した場合に、AP、及びSTAに配送し、更新する場合の手順である。

【0049】図5は、STAとAPとで記憶管理している暗号鍵が4個とも一致しない状態で、STAの記憶管理する暗号鍵を更新する場合の手順を示す。すなわち、例えば、携帯型のSTA装置を長期に渡って帯出し、AP側の暗号鍵が全て更新された後に帯入してAPにアクセスしようとした場合、或いは、あるSTAが長期に渡って移動されることなく放置され、AP側の暗号鍵が全て更新された後に移動された場合などに適用する、暗号鍵更新手順である。

【0050】まず、通常の暗号鍵更新の動作について、図4、及び図1乃至図3を参照して説明する。

【0051】図4において鍵管理サーバは、4個の暗号鍵うち任意の1個(n番)を新たに生成し、鍵管理サーバ内に記憶管理している第n番目の暗号鍵を更新する(n番の鍵更新)と、APに配送(AP鍵配送)する。

【0052】APは鍵管理サーバからAP鍵配送を受けると、AP内に記憶管理している4個の内、第n番目の暗号鍵を更新(n番の鍵更新)し、STAに対して鍵の更新を通知(鍵更新通知)する。この時、APからSTAへ送信される鍵更新通知には、暗号鍵は含まれていない。ただ、APは第n番以外の暗号鍵を用いて、鍵更新通知伝文を暗号化する。

【0053】ここで、鍵管理サーバからAPへ配送された暗号鍵の鍵IDが1(n=1)であるとして、図2を参照して説明する。

【0054】図2を参照すると、鍵管理サーバの有する暗号鍵生成手段200は、新たに暗号鍵を生成すると、APの制御手段201へ配送(AP鍵配送)する。APの制御手段201は、鍵管理サーバから配送された暗号鍵と、鍵ID(1)を暗号鍵設定手段202へ転送する。暗号鍵設定手段202は、制御手段から受け取った暗号鍵を、鍵IDに対応して第1鍵記憶手段203に格納し、更新する。

【0055】次に制御手段201は、平文入力手段21

0と鍵ID生成手段208とを制御して、STAへ鍵の更新を通知する。平文入力手段210は、制御手段からの制御により、鍵更新通知伝文を生成し、WEP暗号化手段211に入力する。鍵ID生成手段208は、更新された鍵のIDとは違うIDを生成する。ここでは、例として鍵ID「2」を出力するものとする。鍵選択手段207は、第2鍵記憶手段204に記憶されている暗号鍵を選択し、WEP暗号化手段211に入力する。IV生成手段209は、鍵IDを2としたIVを生成し、WEP暗号化手段211に入力する。

【0056】WEP暗号化手段211は、IV生成手段209から入力されたIVと、鍵選択手段207から入力された暗号鍵を使用して平文入力手段210から入力される鍵更新通知伝文を暗号化する。暗号文出力手段212は、WEP暗号化手段211の作成した暗号文とIVを入力し、拡張WEPフレームを構成して送信装置などに出力する。

【0057】図4に戻り、STAは、APから鍵更新通知を受けると、AP経由で鍵管理サーバ宛てに鍵の更新を要求する。これを受けて、鍵サーバはSTAの真正性をチェックし、STA鍵配送可と判断すると、AP経由でSTA宛てに暗号鍵を配送する。STAは、鍵管理サーバからSTA鍵配送を受けると、新たな暗号鍵を記憶管理する。

【0058】本発明による無線LANシステムにおいては、STAとAP間の無線区間に以上の手順を採用することによって、より高い安全性を確保している。

【0059】STAが鍵更新通知を受け、鍵の更新を要求する動作について、図3を参照して説明する。

【0060】図3を参照すると、APからの鍵更新通知は、暗号文入力手段313に入力され、IVと暗号文に分けられて復号化手段314に入力される。WEP復号化手段314は、入力されるIVを鍵ID抽出手段316へ出力する。鍵ID抽出手段316は、IV中の鍵IDを取り出して鍵選択手段307を制御する。

【0061】図2の動作説明でIVの鍵IDは「2」としたので、鍵選択手段307は第2鍵記憶手段304を選択する。WEP復号化手段314は、鍵選択手段307の出力する第2鍵を入力されて、鍵変更通知伝文を復号処理する。平文出力手段315は、WEP復号化手段314の復号した平文を出力する。

【0062】制御手段301は、平文出力手段315の出力を参照し、鍵更新通知を検出すると、鍵更新要求伝文を返送する。制御手段301は、鍵ID抽出手段316の出力する鍵IDを参照し、鍵ID生成手段308へ転送する。鍵ID生成手段308は、制御手段から受け取った鍵ID「2」を出力する。鍵選択手段307はこれにより第2鍵記憶手段を選択する。IV生成手段309は、鍵ID「2」のIVを生成する。また、制御手段301は、平文入力手段310を制御して鍵更新要求伝

文を生成する。

【0063】WEP暗号化手段311は、IV生成手段309から入力されたIVと、鍵選択手段307から入力された暗号鍵を使用して平文入力手段310から入力される鍵更新要求伝文を暗号化する。暗号文出力手段312は、WEP暗号化手段311の作成した暗号文とIVを入力し、拡張WEPフレームを構成して送信装置などに出力する。

【0064】次に、STAから鍵更新要求を受けたAPが、鍵管理サーバーへ鍵更新要求伝文を送出し、鍵管理サーバーからのSTA鍵配送をSTAへ送出する動作について、図2を参照して説明する。

【0065】図2において、STAからの鍵更新要求伝文は、暗号文入力手段213に入力され、IVと暗号文に分けられて復号化手段214に入力される。WEP復号化手段214は、入力されるIVを鍵ID抽出手段216へ出力する。鍵ID抽出手段216は、IV中の鍵IDを取り出して鍵選択手段207を制御する。

【0066】STAの送出したIVの鍵IDは「2」であるので、鍵選択手段207は第2鍵記憶手段204を選択する。WEP復号手段214は、鍵選択手段207の出力する第2鍵を入力されて、鍵変更要求伝文を復号処理する。平文出力手段215は、WEP復号化手段214の復号した平文を出力する。

【0067】制御手段201は、平文出力手段215の出力を参照し、鍵更新要求を検出すると、鍵管理サーバーへ鍵更新要求伝文を送出する。

【0068】STAの出力する鍵更新要求伝文には、STA固有の情報を含み、鍵管理サーバーにて鍵配送の可否判断のため、参照される。すなわち、STAは、固有の情報として、STAのMACアドレス、STA使用者の識別情報、パスワードなどを鍵更新要求伝文に含めて送出する。

【0069】鍵管理サーバーはこれらSTAからの固有情報と、予め各STAに関して登録された固有情報とを比較する。そして、受け取った鍵更新要求伝文の送出元STAの真正性が確認された場合に限り、STA宛てに暗号鍵を配送する。

【0070】図2を参照すると、鍵管理サーバーの有する暗号鍵生成手段200は、STA宛ての暗号鍵をAPの制御手段201へ配送（STA鍵配送）する。APの制御手段201は、鍵管理サーバーから配送されたSTA鍵配送伝文を、平文入力手段210に入力する。次に鍵ID生成手段208を制御して、STAへ暗号鍵を配送する。平文入力手段210は、制御手段からのSTA鍵配送伝文を、WEP暗号化手段211に入力する。鍵ID生成手段208は、鍵ID「2」を出力する。鍵選択手段207は、第2鍵記憶手段204に記憶されている暗号鍵を選択し、WEP暗号化手段211に入力する。IV生成手段209は、鍵IDを2としたIVを生

成し、WEP暗号化手段211に入力する。

【0071】WEP暗号化手段211は、IV生成手段209から入力されたIVと、鍵選択手段207から入力された暗号鍵を使用して平文入力手段210から入力されるSTA鍵配送伝文を暗号化する。暗号文出力手段212は、WEP暗号化手段211の作成した暗号文とIVを入力し、拡張WEPフレームを構成して送信装置などに出力する。

【0072】続いて、STAがSTA鍵配送伝文を受け、暗号鍵を更新する動作について、図3を参照して説明する。

【0073】図3を参照すると、APからのSTA鍵配送伝文は、暗号文入力手段313に入力され、IVと暗号文に分けられて復号化手段314に入力される。WEP復号化手段314は、入力されるIVを鍵ID抽出手段316へ出力する。鍵ID抽出手段316は、IV中の鍵IDを取り出して鍵選択手段307を制御する。

【0074】鍵選択手段307は鍵IDに従って、第2鍵記憶手段304を選択する。WEP復号化手段314は、鍵選択手段307の出力する第2鍵を入力されて、STA鍵配送伝文を復号処理する。平文出力手段315は、WEP復号化手段314の復号した平文を出力する。

【0075】制御手段301は、平文出力手段315の出力を参照し、STA鍵配送伝文を検出すると、受け取ったSTA鍵を暗号鍵設定手段302に転送する。暗号鍵設定手段302は、受け取った平文に含まれる、配送された暗号鍵のIDを参照して、対応する鍵記憶手段に格納し、暗号鍵を更新する。この例では、第1鍵を更新するので、平文には鍵ID「1」が含まれる。従って、新たな暗号鍵は第1鍵記憶手段303に格納される。

【0076】以上説明した動作によって、鍵管理サーバーの生成する暗号鍵をAP、及びSTA宛てに配送し、それぞれの記憶管理する暗号鍵を更新することができる。

【0077】次に、多数のSTA、及び、複数のAPに対する、暗号鍵の管理について説明する。

【0078】本発明の無線LANシステムでは、鍵管理サーバーに複数のAPが接続される場合がある。そして、システムに係属するSTAは、フロアレイアウトの変更、または、可搬型STAの移動によって、それまでとは別のAPにアクセスする場合も考えられる。これらの条件に鑑み、複数のAPに加え、多数のSTAの暗号鍵を容易に管理可能とするするため、本発明の無線LANシステムにおいては、鍵管理サーバーは、各AP、STAに配送する暗号鍵を、システム全体に渡って共通の1組（4個）としている。こうすることによって、管理する暗号鍵の数を最小限に留めてシステムの負荷を低減することができる。また、複数のAPに渡ってSTAを移動した場合にも、各APが同一の暗号鍵を有するの

で、暗号鍵不一致の発生を回避することができる。

【0079】次に、本発明の無線LANシステムにおける、暗号鍵の更新、及びSTAとAPにおける暗号鍵の運用について説明する。

【0080】IEEE802.11のWEPでは、4個の暗号鍵を識別して管理、運用することができる。そこで、本発明の無線LANシステムでは、4個の暗号鍵の更新、及び、APとSTAとがそれぞれ通信する場合の暗号鍵の運用について、次に示す幾つかの方法を採用し、高い運用性と情報秘匿性の両立を図っている。

【0081】暗号鍵更新方法の第1として、鍵管理サーバーは、4個の暗号鍵をある一定の期間が経過するごとに、1個ずつ順次更新していく。具体的には、1週間経過する毎に、1個ずつ順次更新する。こうすることによって、それぞれの暗号鍵は4週間に1度、更新されることとなる。従って、携帯型のSTAを帯出する者は、4週間以内にSTAを帯入すれば、問題無くAPにアクセスすることができる。

【0082】この期間の長さは、鍵管理サーバーにて設定可能としてもよく、システムの要求によって、例えば1日毎、1ヶ月毎などとしてもよい。

【0083】この要領で暗号鍵を更新するシステムでは、STAとAPは次に示す、幾つかの方法で暗号鍵を運用する。

【0084】その1によれば、APは4個の暗号鍵の内、最後に更新した暗号鍵を通信に使用せず、他の3個を順次用いてSTAと通信する。

【0085】複数のSTAが存在するシステムにおいては、全てのSTAの記憶管理する暗号鍵の更新には時間を要する。すなわち、暗号鍵の更新は鍵管理サーバーからAP、STAに対して個別に行われるため、APが暗号鍵を1個更新した時、各STAはAPからの暗号鍵更新通知を受けて逐次鍵管理サーバーへ暗号鍵更新要求を行い、鍵管理サーバーから鍵配送を受けて個々に暗号鍵を更新する。

【0086】この方法を採用することによって、APが1個の暗号鍵を更新してから、全てのSTAの記憶管理する暗号鍵の更新が完了するまでの間、暗号鍵の不一致に起因する障害を回避することが可能となる。

【0087】その2によれば、APは、最初に更新した暗号鍵を用いてSTAと通信する。

【0088】こうすることによって、STAはより長い期間に渡って暗号鍵更新の機会を得ることができる。

【0089】上記第1の暗号鍵の更新方法における、その1、及びその2の暗号鍵の使用法において、STAは、STAの記憶管理する暗号鍵の内、最後に更新されたものを使用して通信する。こうすることによって、携帯型STAの帯出可能期間、あるいはSTAの非稼働可能期間を最も長くすることができる。尚、情報秘匿性向上のために、最後に更新された暗号鍵以外の暗号鍵を適

宜利用してもよい。

【0090】暗号鍵更新方法の第2として、鍵管理サーバーは、特定の暗号鍵の更新周期を他の暗号鍵の更新周期よりも大幅に長く設定し、他の暗号鍵はより短い更新周期で順次更新する。具体的には、第1の暗号鍵は3ヶ月毎に更新し、第2乃至第4の鍵については、1日毎に1個ずつ順次更新する。こうすることによって、携帯型のSTAを帯出する者は、3ヶ月以内にSTAを帯入すれば、問題無くAPにアクセスすることができるので、利便性が向上するとともに、他の3個の暗号鍵は3日周期で更新されるため、これを通信に利用すれば情報秘匿性は向上する。

【0091】尚、この方法においても、暗号更新周期は、システムの要求によって、任意に定められてよいことは、言うまでも無い。

【0092】この要領で暗号鍵を更新するシステムでは、STAとAPは次に示す、幾つかの方法で暗号鍵を使用することができる。

【0093】その1によれば、APは3日周期で更新される暗号鍵を適宜使用して、STAと通信する。APと一致した暗号鍵を記憶管理しているSTAも、3日周期で更新される暗号鍵を使用して通信することで、STAとAP間の通信における情報の秘匿性は高く保つことができる。しかしながら、STAが3日以上帯出された後、帯入されてAPにアクセスする場合、あるいは、3日以上非稼働状態にあったSTAが再度稼働されてAPにアクセスする場合には、暗号鍵の不一致を生じる。この場合APは、その2に示す方法により、STAと通信する。

【0094】その2によれば、APはSTAからの伝文の暗号鍵が、APにて記憶管理するものと不一致を生じた場合、3ヶ月周期で更新する暗号鍵を用いてSTAとの通信を試みる。この方法で暗号鍵が一致した場合、APはSTAに対して暗号鍵の更新を通知する。STAはこれにより暗号鍵更新要求を行い、鍵管理サーバーから最新の暗号鍵を配送され、更新することができる。

【0095】ところで、上記第2の暗号鍵更新方法を用いても、3ヶ月を超えて長期に渡るSTAの帯出、あるいは非稼働に対しては、全ての暗号鍵が不一致となる。

【0096】次に、このような場合の暗号鍵更新動作について、図5を参照して説明する。

【0097】図5を参照すると、APと一致する暗号鍵を有しないSTAは、例えば第1鍵から順次STAにて記憶管理している暗号鍵を使用して、APにアクセスを要求（アクセス要求1回目）する。APは、暗号鍵が一致しないので、平文を使用して鍵の不一致を通知（鍵NG通知1回目）する。

【0098】暗号鍵の不一致を4回繰り返すと、STAは平文を利用して、鍵の一括更新を要求（鍵の一括更新要求）する。APは、STAからの鍵の一括更新要求を

鍵管理サーバーへ転送する。このとき、暗号鍵の一括更新要求伝文には、STAの個別情報が含まれることは、図4にて説明した動作と同様である。

【0099】鍵管理サーバーはSTAの個別情報をチェックし、真正性を確認すると、AP経由でSTA暗号鍵を一括して配送する。STAは鍵管理サーバーからのSTA暗号鍵一括配送を受けると、記憶管理していた暗号鍵を一括して更新する。

【0100】次にSTAは、新たな暗号鍵を使用してAPにアクセスを要求する。APは暗号鍵を確認し、一致すると、通常のデータ通信を開始する。

【0101】尚、図5は、理解の容易のためSTAは4回に渡ってアクセス要求するものとしているが、より効率的なシーケンスも考えられることは言うまでも無い。すなわち、STAは4個の暗号鍵の内、最後に更新された暗号鍵を第1回目のアクセス要求に使用し、これが不一致となった場合には、直ちに鍵の一括更新を要求する、などのシーケンスが考えられる。

【0102】ところで、図5のシーケンスチャートにおいて、STAの暗号鍵一括更新要求からSTA暗号鍵一括配送までの、STAとAP間の無線通信は、平文で行うものとしている。これは、図5は、APとSTAの間の無線区間を含む、別途の暗号化通信を適用することを前提としているためである。

【0103】すなわち、図5上部に示すように、鍵管理サーバーからSTAまでの区間において、あるいは、APからSTAまでの区間において、公開鍵を使用するなどにより、本発明とは別途の暗号化復号化を併用することで、図5のシーケンスにおいて安全にSTAの暗号鍵を更新することが可能となる。

【0104】本発明によれば、STAの記憶管理する4個の暗号鍵の全てがAPと一致しない状態となっても、無線LANシステムによって暗号鍵を一括更新する（すなわち、人間系によって暗号鍵をSTAに設定するなどの作業を介さずに暗号鍵を更新可能とする）ことができる。

【0105】

【発明の効果】以上説明したように本発明によれば、1以上のAPとLANで接続された鍵管理サーバー装置を有し、全てのAPとSTAの間の暗号化無線通信に使用する暗号鍵を1組（k個）とし、鍵管理サーバー装置にて一元的に管理することによって、暗号鍵の管理のために装置の回路規模が増大することもなく、また、暗号鍵の管理のために処理の負荷が増大することもなく、容易に1対多の無線LANシステムを提供することができる。

【0106】また、本は発明によれば、可搬型のSTAを使用者が持ち運んで移動したり、フロアのレイアウト変更などによってSTAが移設されることによって、それまでとは異なるAPにアクセスすることとなった場合

にも、STAと、STAのアクセスするAPとの間で記憶管理している暗号鍵が不一致となることがない、無線LANシステムを提供することができる。

【0107】さらに、本発明によれば、可搬型のSTAを使用者が長期に帯出したためにSTAの暗号鍵の更新がされず、再度帯入した時にはSTAの記憶していた全ての暗号鍵が、アクセスしたAPと不一致する状態となった場合にも、STAに対する暗号鍵の更新手順を提供するので、人間系の操作による煩雑な対応処置を必要とせずにSTAの記憶していた暗号鍵を更新できる、高い運用性を有する暗号通信方式を提供することができる。

【図面の簡単な説明】

【図1】本発明の無線LANシステムの構成を示すブロック図である。

【図2】本発明のAPの構成を示すブロック図である。

【図3】本発明のSTAの構成を示すブロック図である。

【図4】本発明の暗号鍵更新手順を説明するためのシーケンスチャートである。

【図5】本発明の暗号鍵更新手順を説明するためのシーケンスチャートである。

【図6】従来の技術において、IEEE802.11のWEPによる暗号化方式を説明するためのブロック図である。

【図7】従来の技術において、IEEE802.11のWEPによる復号化方式を説明するためのブロック図である。

【符号の説明】

101 鍵管理サーバー

102 AP

103 STA

200 暗号鍵生成手段

201 制御手段

202 暗号鍵設定手段

203 第1鍵記憶手段

204 第2鍵記憶手段

205 第3鍵記憶手段

206 第4鍵記憶手段

207 鍵選択手段

208 鍵ID生成手段

209 IV生成手段

210 平文入力手段

211 WEP暗号化手段

212 暗号文送出手段

213 暗号文入力手段

214 WEP復号化手段

215 平文出力手段

216 鍵ID抽出手段

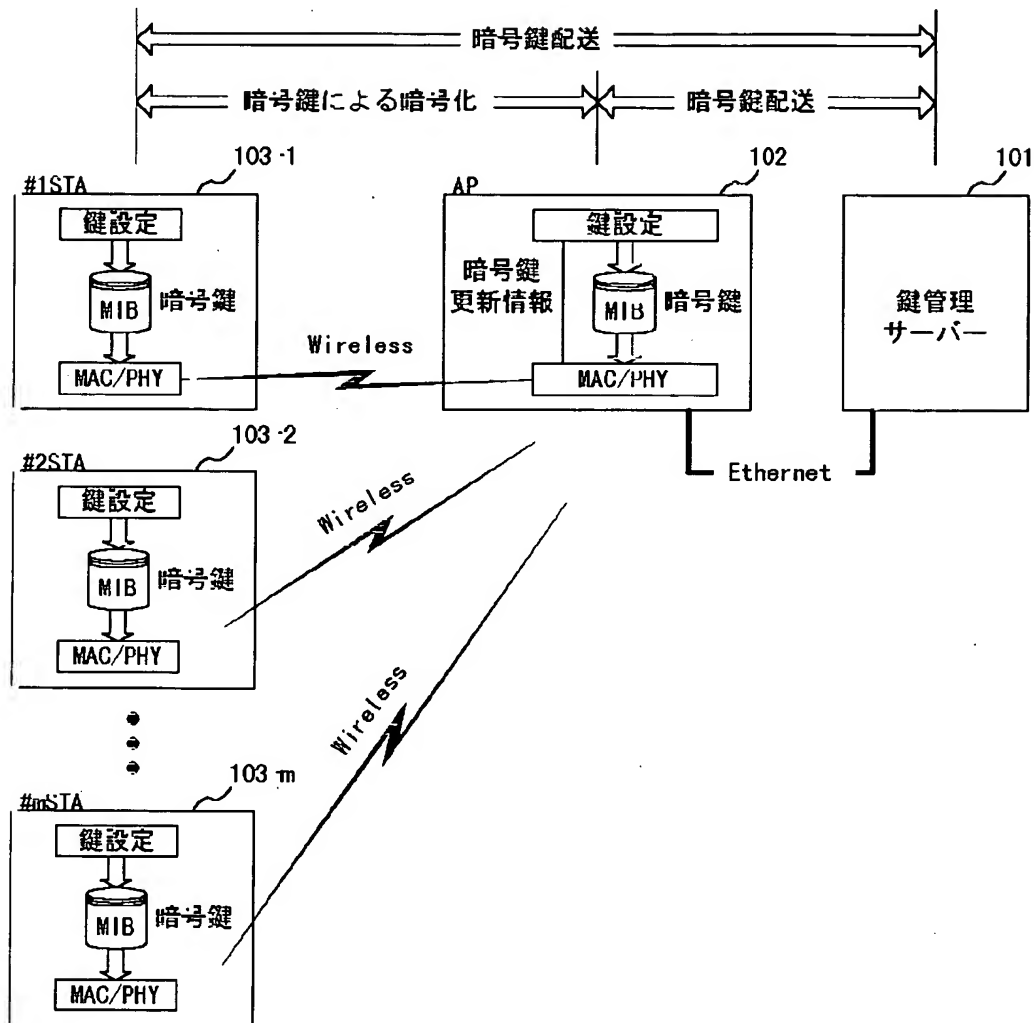
301 制御手段

302 暗号鍵設定手段

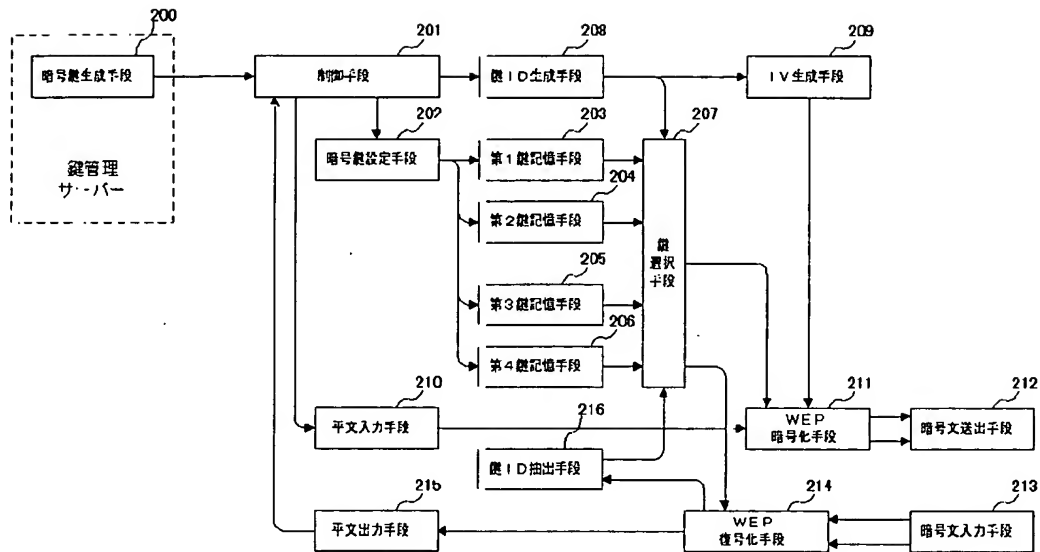
303 第1鍵記憶手段
 304 第2鍵記憶手段
 305 第3鍵記憶手段
 306 第4鍵記憶手段
 307 鍵選択手段
 308 鍵ID生成手段
 309 IV生成手段

310 平文入力手段
 311 WEP暗号化手段
 312 暗号文送出手段
 313 暗号文入力手段
 314 WEP復号化手段
 315 平文出力手段
 316 鍵ID抽出手段

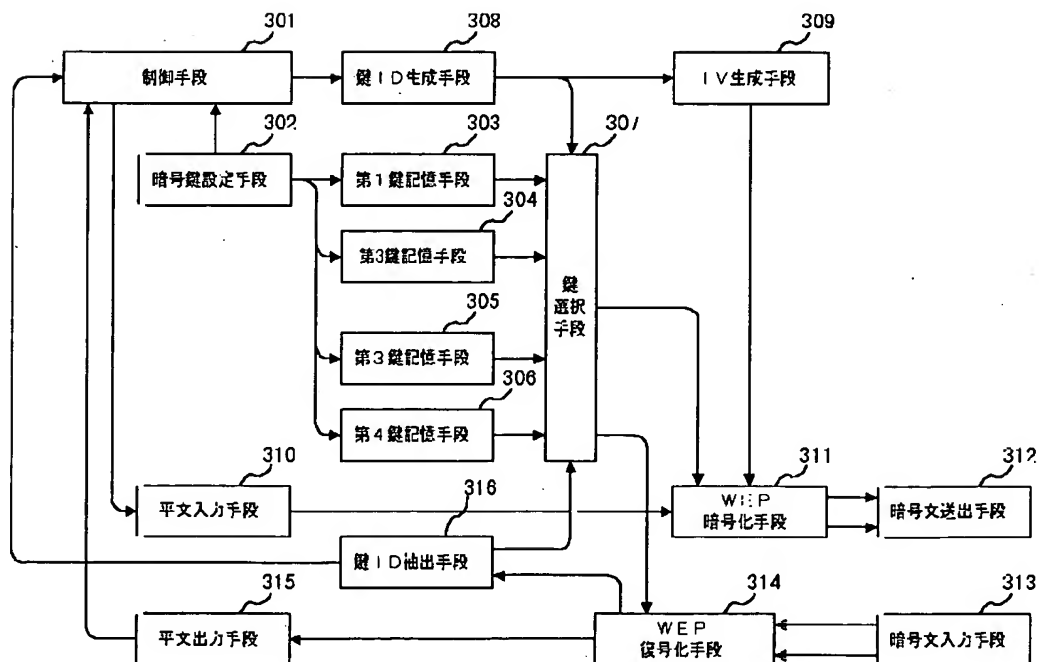
【図1】



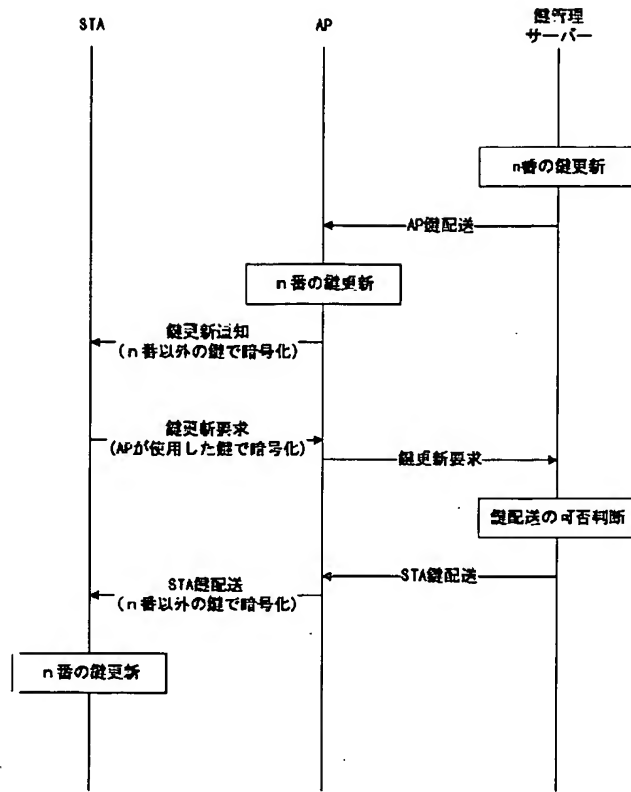
【図2】



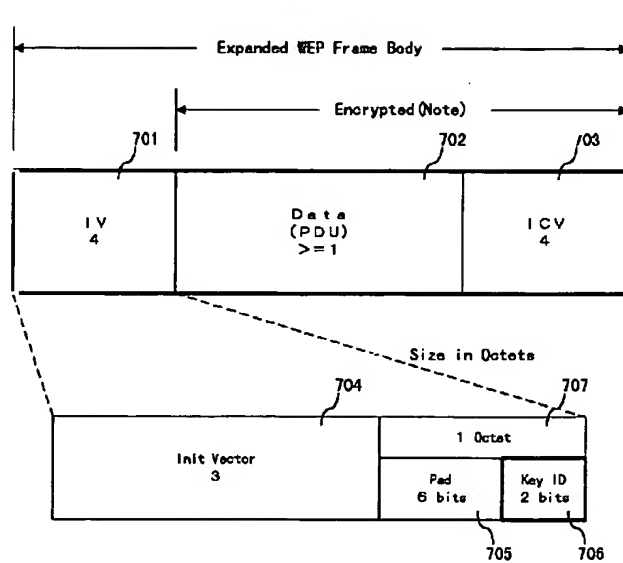
【図3】



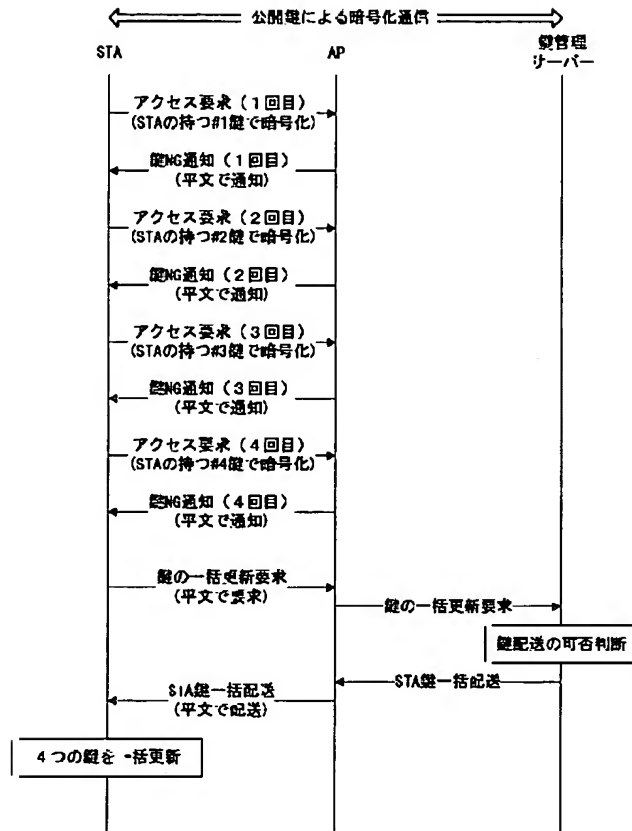
【図4】



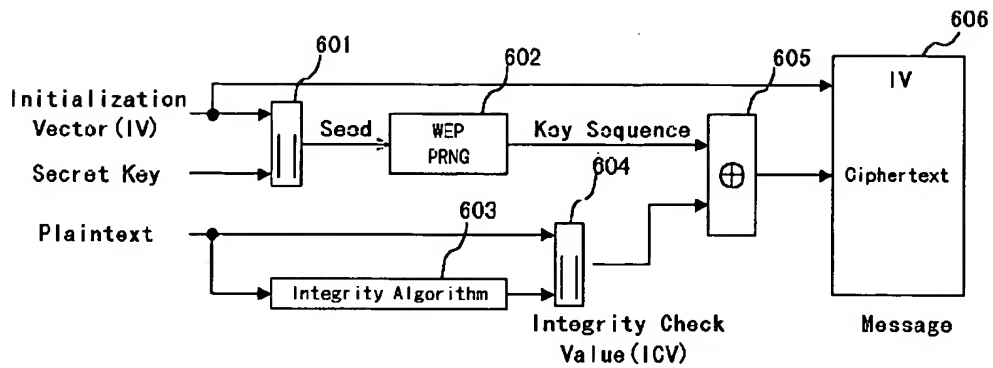
【図7】



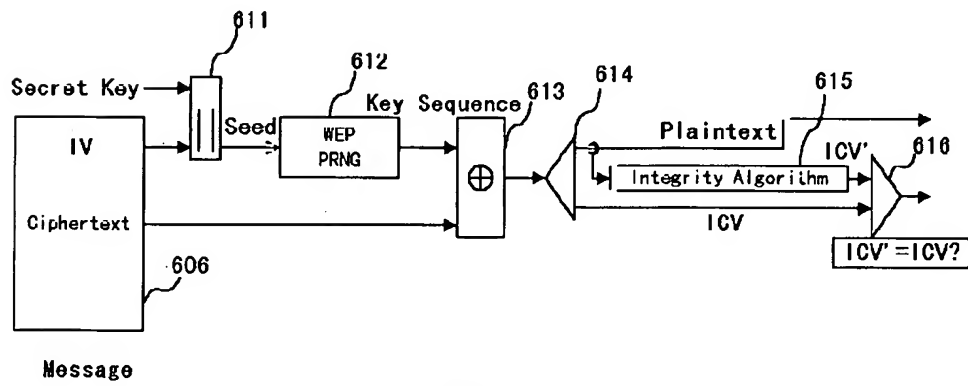
【図5】



【図6】



(a)



(b)